<u>REMARKS</u>

Status of Claims

This application has been reviewed in light of the Office Action dated December 7, 2005. Claims 1-29 are presented for examination. Claims 1, 4, 7, 10, 13, 14, 16, 18, and 20-29, which are independent claims, have been amended as discussed below. Claim 11 has also been amended for consistency of claim language. Favorable reconsideration is requested.

Summary of Interview

Applicants would like to thank the Examiner for granting and conducting an interview on April 27, 2006 at the U.S.P.T.O. with Applicants' representative. The substance of that interview is summarized in the Examiner's Interview Summary (mailed May 10, 2006). Additional details of the arguments presented at that interview are set out in the following.

Rejections Under 35 U.S.C. § 101

Claims 7, 8, 10, and 13 were rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. These claims have been amended to include the phrase "embodied in a computer-readable medium," as suggested by the Examiner. Accordingly, it is believed that these rejections have been obviated and their withdrawal is therefore respectfully requested.

Rejection Under 35 U.S.C. § 112

        Claim 22 has been amended to ensure antecedent basis for the term "second target host," in response to the rejection under 35 U.S.C. § 112, second paragraph. Accordingly, it is believed that this rejection has been obviated and its withdrawal is therefore respectfully requested.

Rejections Under 35 U.S.C. § 102(a)

        Claims 1-29 have been rejected under 35 U.S.C. § 102(a) as being anticipated by Kargl, Frank, et al., "Protecting Web Servers From Distributed Denial of Service Attacks" ("Kargl").

        While anticipation is not an *ipsissimis verbis* test, it is well-established that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." M.P.E.P. § 2131 (quoting *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)). Moreover, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." M.P.E.P. § 2131 (quoting *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)).

Kargl

        Kargl relates to protecting web servers from distributed denial of service (DDos) attacks. Denial of service attacks are designed to overload a computer or a computer network to render them incapable of providing normal services (see Kargl at

Section 2.2). A "distributed" attack uses multiple computers to launch a coordinated denial of service attack   A "master" or "handler" program is installed in a computer system, which communicates with multiple "daemon" or "agent" programs installed on computers throughout the Internet. The DDoS master and daemon programs are "pre-compiled binaries" (i.e., object or executable code) that perform a <u>fixed, limited set of pre-programmed functions</u> (see Kargl at Section 2.4). Upon receiving a predetermined command, or at a predetermined time, the agents begin to attack the target computer or network, usually by directing connection requests or other forms of network communication toward the targeted system.

Claims 1, 4, 7, 14, 16, and 18

Claim 1 is directed to a system for performing penetration testing of a target computer network by installing a remote agent in a target host of the target computer network. The system includes a local agent provided in a console and configured to receive and execute commands. A user interface is provided in the console and is configured to send commands to and receive information from the local agent, process the information, and present the processed information. A database is configured to store the information received from the local agent. A network interface is connected to the local agent and configured to communicate via a network with the remote agent installed in the target host of the target computer network. The system further includes security vulnerability exploitation modules for execution by the local agent and/or the remote agent. The remote agent comprises at least one of: a system-calls proxy server configured to

receive and execute, in the target host, system calls received via the network, and a virtual

machine configured to execute, in the target host, scripting language instructions received

via the network.

Among the advantages provided by these claimed features is the ability of

the system-calls proxy server to remotely execute complex programs as if they were

resident on the target host itself:

> [0074] By acting as a syscall proxy, the remote agent 120
> allows the local agent 135 to execute commands as if the
> local agent 135 were resident on the first target host 115.
> The syscall proxy configuration allows large, complex
> programs, such as the automated penetration testing program
> resident on the console 105, to execute system calls on a
> target host without actually being resident on the target host.
> Only the relatively small agent needs to be installed on the
> target host.

The virtual machine provides similar advantages:

> [0081] One advantage of executing modules in a virtual
> machine 310 is that it allows the level 2 agent 305 to perform
> computationally-intensive operations on the target host 210
> without receiving a continuous flow of instructions, as in the
> case of syscall proxying. Indeed, syscall proxying may not
> be feasible for computationally-intensive operations because
> of the delays in transmitting instructions that result from
> network latency. Thus, the virtual machine 310 of the level 2
> agent 305 can take greater advantage of the processor and
> other resources of the target host 210.

Even if Kargl's daemons are considered to be remote agents, nothing has

been found or pointed out in Kargl that would teach or suggest a remote agent that

comprises "at least one of: a system-calls proxy server configured to receive and execute,

in the target host, system calls received via the network, and a virtual machine configured

to execute, in the target host, scripting language instructions received via the network," as

recited in Claim 1. To the contrary, Kargl is silent as to the structure of the daemons and has only minimal discussion of their functionality. Kargl merely discusses the capability of the daemons to perform rudimentary communication with the master programs and to direct certain predetermined types of network communications toward a target network.

The Examiner states that "routers and firewalls clearly encompass proxy servers, as broadly interpreted by the Examiner." (Office Action at page 10. However, these network components do not constitute part of a remote agent installed in the target host, in the manner claimed. Similarly, the Examiner states that "web based servers are JAVA capable such that a virtual machine is inherently part of the JAVA functionality, as broadly interpreted by the Examiner." (Office Action at page 10). Even if such capabilities are present in the target host, as the Examiner hypothesizes, they do not constitute part of a remote agent installed in the target host, in the manner claimed. It is therefore respectfully submitted that Kargl does not disclose the "identical invention" to that claimed.

Accordingly, Claim 1 is believed to be patentable over Kargl. Independent Claims 4, 7, 14, 16, and 18 recite features similar to those discussed above with respect to Claim 1 and therefore are also believed to be patentable over Kargl for the reasons discussed above.

Claims 10 and 13

Claim 10 is directed to an agent embodied in a computer-readable medium for use in a system for performing penetration testing of a target computer network having

a target host. The agent includes a system-calls proxy server configured to receive and execute, in the target host, system calls received via a network. The agent further includes a virtual machine configured to execute, in the target host, scripting language instructions received via the network. The system calls received via the network are routed to the system-calls proxy server, and the scripting language instructions received via the network are routed to the virtual machine.

As discussed above, Kargl does not teach or suggest an agent comprising a system-calls proxy server or a virtual machine, much less an agent comprising both, as recited in Claim 10. Nor does Kargl teach or suggest an agent in which system calls received via the network routed to a system-calls proxy server, and scripting language instructions received via the network are routed to a virtual machine, as further recited in Claim 10.

Accordingly, Claim 10 is believed to be patentable over Kargl. Independent Claim 13 recites features similar to those discussed above with respect to Claim 10 and therefore is also believed to be patentable over Kargl for the reasons discussed above.

In addition, Claim 13 recites the following elements for which no corresponding structures have been identified in Kargl, or elsewhere in the prior art. Claim 13 recites a secure communication module configured to provide secure communication between the virtual machine and the network; an execution engine configured to control the system-calls proxy server and the virtual machine, wherein the system calls and the scripting language instructions are routed to the system-calls proxy server and the virtual machine, respectively, by the execution engine; and a remote

procedure call module configured to receive commands via the network formatted in a remote procedure call protocol and pass the commands to the execution engine; and a second secure communication module configured to provide secure communication between the remote procedure call module and the network.

The Examiner states that root kits, as mentioned in Section 2.4 of Kargl, "inherently involve the interception of operating system calls at the kernel level." (Office Action at page 13). However, Claim 13 recites that the "agent includes a system-calls proxy server configured to <u>receive and execute</u>, in the target host, <u>system calls received via a network</u>." By contrast, root kits, like the daemons discussed in Kargl, are merely precompiled code that execute certain preprogrammed functions, while seeking to hide such execution. The bare idea of a root kit does not teach or suggest an agent having a system-calls proxy server for receiving and executing system calls, in the manner claimed.

Accordingly, it is submitted that anticipation of Claim 13 by Kargl has not been established and withdrawal of this rejection is therefore respectfully requested.

Claims 20-29

Claim 20 is directed to a method for performing penetration testing of a target network. The method includes the step of executing a first module to exploit a security vulnerability of a first target host of the target network. A first remote agent is installed in the first target host as a result of exploiting the security vulnerability of the first target host. A system call is sent to the first remote agent via a network. The system call is executed in the first target host using a system-calls proxy server of the first remote agent

- 23 -

to exploit a security vulnerability of a second target host. The system call comprises a computer instruction that is executed in an operating system of the first target host.

As discussed above, Kargl does not teach or suggest a remote agent having a system-calls proxy server installed in a target host. *A fortiori*, Kargl does not teach or suggest a remote agent capable of executing a system call comprising a computer instruction that is executed in an operating system of the first target host, as recited in Claim 20.

Accordingly, Claim 20 is believed to be patentable over Kargl. Independent Claims 21-29 recite features similar to those discussed above with respect to Claim 20 and therefore are also believed to be patentable over Kargl for the reasons discussed above.

Dependent Claims

The other claims in this application are each dependent form one or another of the independent claims discussed above and are therefore believed patentable for the same reasons. Since each dependent claim is also deemed to define an additional aspect of the invention, however, the individual consideration of the patentability of each on its own merits is respectfully requested.

Conclusion

In view of the foregoing amendments and remarks, Applicants respectfully request favorable reconsideration and early passage to issue of the present application.

Applicants' undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,

Carl B. Wischhusen
Attorney for Applicants
Registration No. 43,279

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

NY_Main 569617_2